However, Bellisent does not explicitly indicate mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets.

Valdya teaches mapping the traffic flow to a memory space by applying a hash function (col 3, lines 27-48; col 9, lines 3-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Valdya into those of Belissent in order to make the system more organized. The organization of the system using a hash function is known in the art. A specific hash function is used because its backward computation is difficult as well as its tendency to be collision free.

Applicant's claim 1 is distinct over the combination of Belissent and Valdya. Claim 1 calls for producing statistics corresponding to a parameter of traffic flow to trace the source of an attack. Without conceding that Belissent teaches this feature of the invention, namely that "the client's request rate" teaches the feature of producing statistics corresponding to a parameter of traffic flow to trace the source of an attack, Belissent taken with Valdya fail to suggest mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow ... accumulating statistics ... comparing the number of buckets to a threshold, and determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold.

The examiner contends that Belissent teaches these features at col. 2, line 49 to col. 3, line 36; by the teaching that: "the rate of connections is compared to thresholds and appropriate action is taken)." This is incorrect.

It is clear that Belissent fails to suggest ... mapping the traffic flow into a plurality of buckets ... accumulating statistics ... comparing the number of buckets to a threshold, and determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold.

In Belissent, at the cited passage and elsewhere, Belissent merely suggests to measure the number of connection requests over a time period and if the number of connection requests is above a threshold, either waiting for a period before accepting the connection request, to throttle the client making the request, or simply rejecting the connection request. Belissent fails to suggest accumulating statistics on traffic flow and fails to map that traffic flow into a plurality of buckets. Moreover, in Belissent the action resulting from determining a rate of connection requests is to allow or deny, or throttle the connection requests.

Belissent is utterly void of any teachings that dynamically reconfigure a number of buckets that are used to track statistics of traffic flow based on one or more buckets exceeding or being under a threshold. To the extent that the examiner considers determining rates of connection requests as buckets, Belissent does not change the number of buckets based on one or more buckets exceeding or being under a threshold.

The examiner uses Valdya to teach hashing. Applicant contends that Valdya fails to suggest "mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow." While Valdya indeed mentions the use of a "hash index" to access a cache, Valdya fails to suggest to apply any hash to a parameter of traffic flow or to use the hash to map traffic into a plurality of buckets. Applicant does not profess to be the originator of hash functions, but rather has used the hash function in a technique to map traffic flow into buckets. Valdya uses the hash to search a cache for matching session entries in the cache, a common technique employed to distribute entries in a cache memory. However, Valdya adds no further teachings to cure the deficiencies in Belissent and therefore Belissent taken together or separately from Valdya fails to suggest claim 1.

Claims 14, 21, 63, and 70 recite additional implementations and are allowable at least because they include the feature of compare the accumulated statistic values from the buckets to configured threshold values corresponding to the number of buckets to determine that an event is of significance (claim 14) or adjust the number of buckets as the number of buckets approaches a second threshold (claim 21). Claims 63 and 70 are allowable because they recite the feature of "varying the number of buckets according to the amount of traffic and number of flows according to down traffic flow into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in the bucket." Neither of the cited references suggest at least these features of these claims.

As to claim 3, Belissent fails to suggest that as the number of buckets changes, the buckets have values derived from the buckets prior to the change. The examiner contends that this is taught at (col. 2, line 49 to col.. 3, line 36). No such teachings are found at that passage, as discussed above.

As to claim 4, the examiner contends that Valdya teaches that the hash function adapts to map to the new number of buckets, as the new number of buckets changes. (col. 9, lines 3-45).

Valdya fails to teach a hash function to "mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow," as in claim 1 and further fails to teach that the hash function changes, as the number of buckets change. The examiner fails to show how a hash index to access a cache system, as taught by Valdya, has any relation to using a hash function to map statistics to buckets, that the hash function adapts to map to the new number of buckets, as the new number of buckets changes, as in claim 4.

As to claim 5, Belissent fails to teach that comparing statistic values includes comparing the value accumulated in the bucket to a threshold that depends on the number of buckets. (col. 2, line 49 to col. 3, line 36). Rather, Belissent merely teaches to compare connection requests to a threshold but that threshold is not dependent on a number of buckets used to track packet statistics.

As to claim 6, Belissent fails to teach that the parameter is the count of how many packets a data collector or gateway examines at col. 5, lines 4-20 or elsewhere. Belissent mentions IP and TCP protocols but fails to suggest tracking a count of the number of packets examined by a data collector or gateway.

As to claim 7, Belissent fails to teach that as a value of a parameter for one bucket approaches a threshold, the monitoring device raises an alarm at col. 2, line 49 to col. 3, line 36 or elsewhere. Belissent merely teaches that as the number of connection requests reach a threshold that the number of connection requests are granted are throttled, e.g., reduced. Belissent fails to suggest raising an alarm.

As to claim 8, Valdya fails to teach that the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets at col. 9, lines 3-45 or elsewhere. As Valdya uses a hash to form a hash index to access a cache, it seem illogical that Valdya would change the hash in a random, secret manner. Valdya fails to mention this and the examiner has failed to show how or why Valdya would want to use a secret hash to produce a hash index.

As to claim 9, Belissent fails to teach that the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored, so that the monitoring device is not vulnerable to a denial of service attack against its own resources at col. 2, line 49 to col. 3, line 36) or elsewhere.

As to claim 10, Belissent fails to teach that the variable number of buckets efficiently identifies the source or sources of attack by breaking down traffic into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in each bucket (col. 4, lines 9-25) or elsewhere. Belissent, unlike Applicant, is directed at the relatively limited problem of trying to minimize a Denial of Service attack. Applicant on the other hand is directed to tracking the flows, in order to identify the source or sources of an attack. Belissent's technique is limited to situations where the source of the attack is identified, Col. 2 lines 23-26. Belissent improves on the stated conventional technique by throttling such connection requests rather than completely rejecting them. However, this technique is not useful against spoofing attacks. Applicant's on the other hand seeks to determine unusual amounts and types of network traffic statistics, so as to determine the actual sources of the attack.

As to claim 11, Belissent fails to teach that the traffic is monitored at multiple levels of granularity, from aggregate to individual flows at col. 3, lines 6-36 or elsewhere.

As to claim 12, Belissent fails to teach that monitoring of TCP packet ratios and repressor traffic at col. 5, lines 20-35 or elsewhere.

As to claim 13, Belissent fails to teach that the threshold is a first threshold and the method further comprises: comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance at col. 5, lines 45-52) or elsewhere.

Claims 15-20, 50-62, 64-69, and 71 -77 are allowable at least for the reasons discussed in their respective base claims.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

In view of the foregoing remarks, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

No fee is believed due. Please apply any charges to deposit account 06 1050, referencing attorney docket 12221-007001. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 12/14/05

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21213189.doc